

ABSTRACT

Method and system for copy protecting information from a service provider, which is transmitted between a point of deployment (POD) module and a set-top box, are disclosed by an arrangement in which control information pairs are transmitted from the POD module to the set-top box. The control information pairs are respectively associated with the portions of the copy protected information, for example, elementary streams, transmitted between the POD module and host device. To prevent hackers or an intruder from tampering with the copy protected information, the control information pairs are incorporated into a shared key calculation in the POD module and set-top box. The shared keys are used by the POD module and set-top box to encrypt and decrypt the information (e.g. elementary streams). If the at least one control information pair is tampered with during transmission between the POD module and the set-top box, then the shared key(s) calculated by the set-top box and POD module will not match, and the set-top box will not be able to correctly decrypt the encrypted information received from the deployment module.